Cyber Security in the Electric Sector

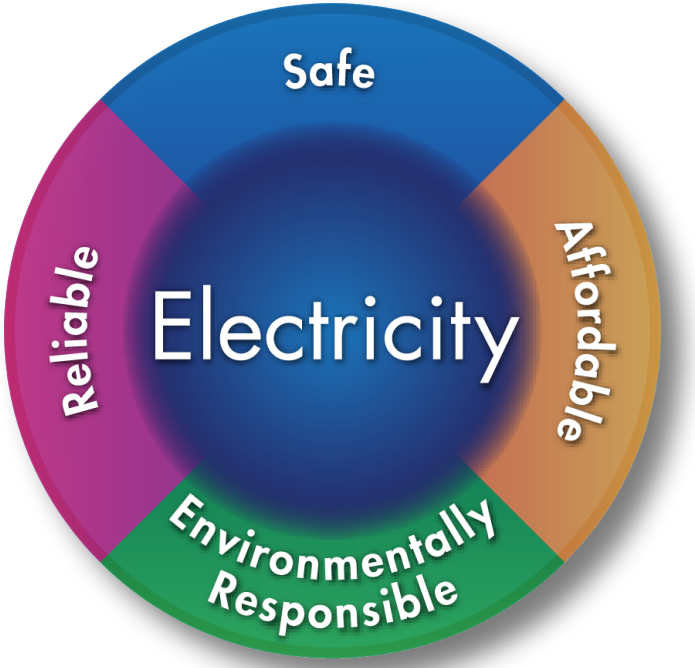
Annabelle Lee

Principal Technical Executive
Electric Power Research Institute (EPRI)

alee@epri.com
202.293.6345

EPRI's Mission

Advancing ***safe***, ***reliable***, ***affordable,*** and ***environmentally responsible*** electricity for society through global collaboration, thought leadership and science & technology innovation



Three Key Aspects of EPRI

Independent

Objective, scientifically based results address reliability, efficiency, affordability, health, safety, and the environment

Nonprofit

Chartered to serve the public benefit

Collaborative

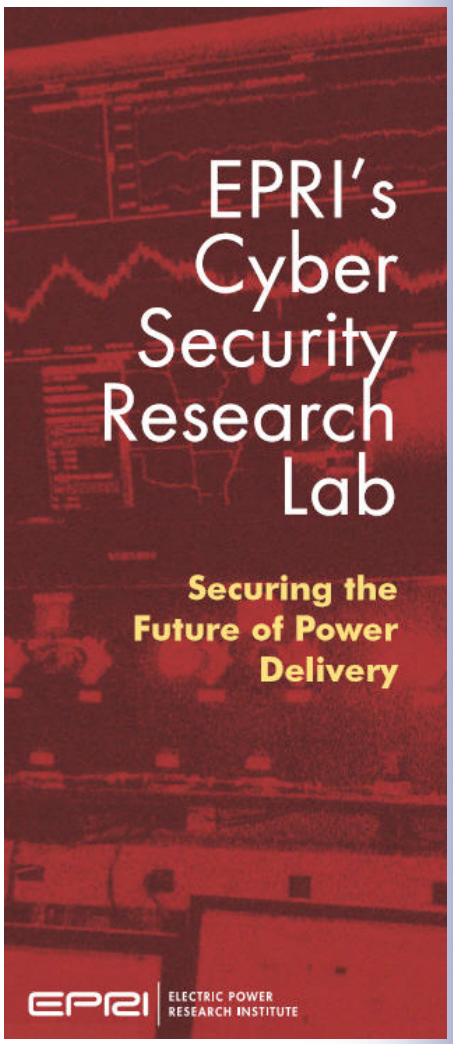
Bring together scientists, engineers, academic researchers, and industry experts

Our Members…

- 450+ participants in more than 30 countries
- EPRI members generate approximately 90% of the electricity in the United States
- International funding – nearly 25% of EPRI's research, development, and demonstrations

EPRI Cyber Security Research

- Technology Transfer
- Industry Coordination
- Transition to Practice



Before we continue let's get over our fears and myths with some much needed levity …

Thanks to Daniel Thanos, VP of Lookout for the following slides

Sum of All Myths

Wishful Immunity

Myth: **There is no problems here** just happy and trusted people working on reliable and isolated systems

Fact: **Sophisticated attackers use trusted people and privileged access** without the target's knowledge

They usually succeed when security is exclusively perimeter and "trust" based

Sum of All Myths

Mordac Syndrome

Myth: **Security reduces reliability** and degrades capabilities and prices us out of existence

Fact: **Correctly engineered security increases reliability** and reduces costs and risks due to poor design and systemic failures

The Sum of All Fears

Point and Click Attacks

Fear: **All generators and transformers can be cyber-attacked** with script kiddie ease!

Fact: **There are more interlocked safeties, backups, and other secondary systems and processes** that make these cyber-attacks more difficult in practice

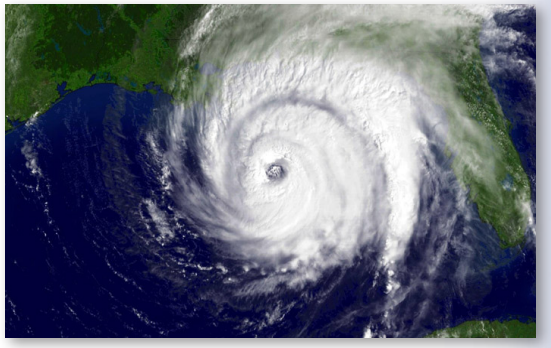
Need to concentrate on enhancing existing safety and reliability practices to address cyber security risks

Background

Threats to the Grid

- Deliberate attacks
  - Disgruntled employees
  - Industrial espionage
  - Unfriendly states
  - Organized crime
  - Terrorists

- Inadvertent threats
  - Equipment failures
  - User/Administrator errors



- Natural phenomena
  - Weather – hurricanes, earthquakes
  - Solar activity

Trends Impacting Security

- Increasing reliance on automation

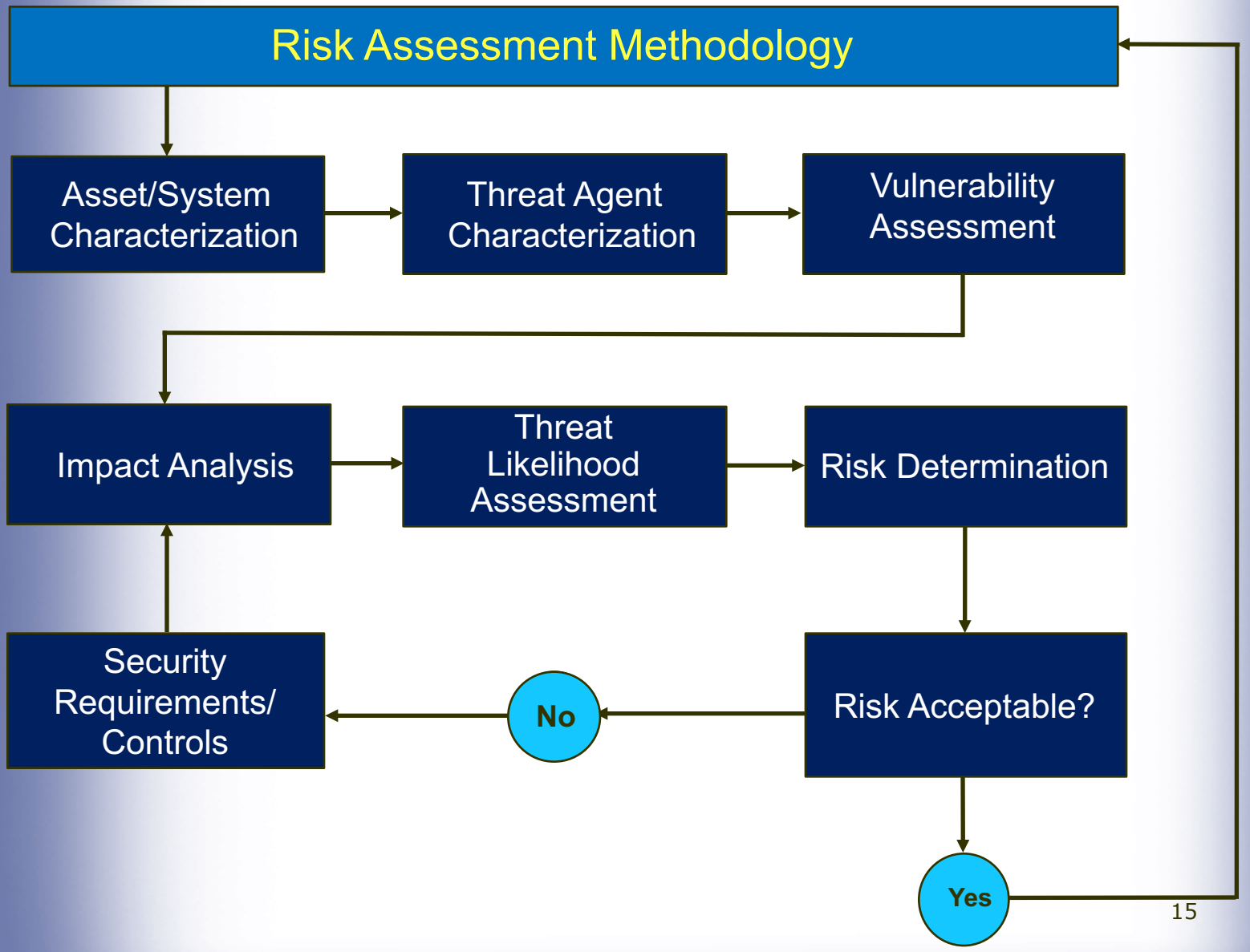
- Open protocols
  - Open industry standard protocols are replacing vendor-specific proprietary communication protocols
- Common operating systems
  - Standardized computer platforms increasingly used to support control system applications
- Interconnected to other systems
  - Connections with enterprise networks to obtain productivity improvements and information sharing

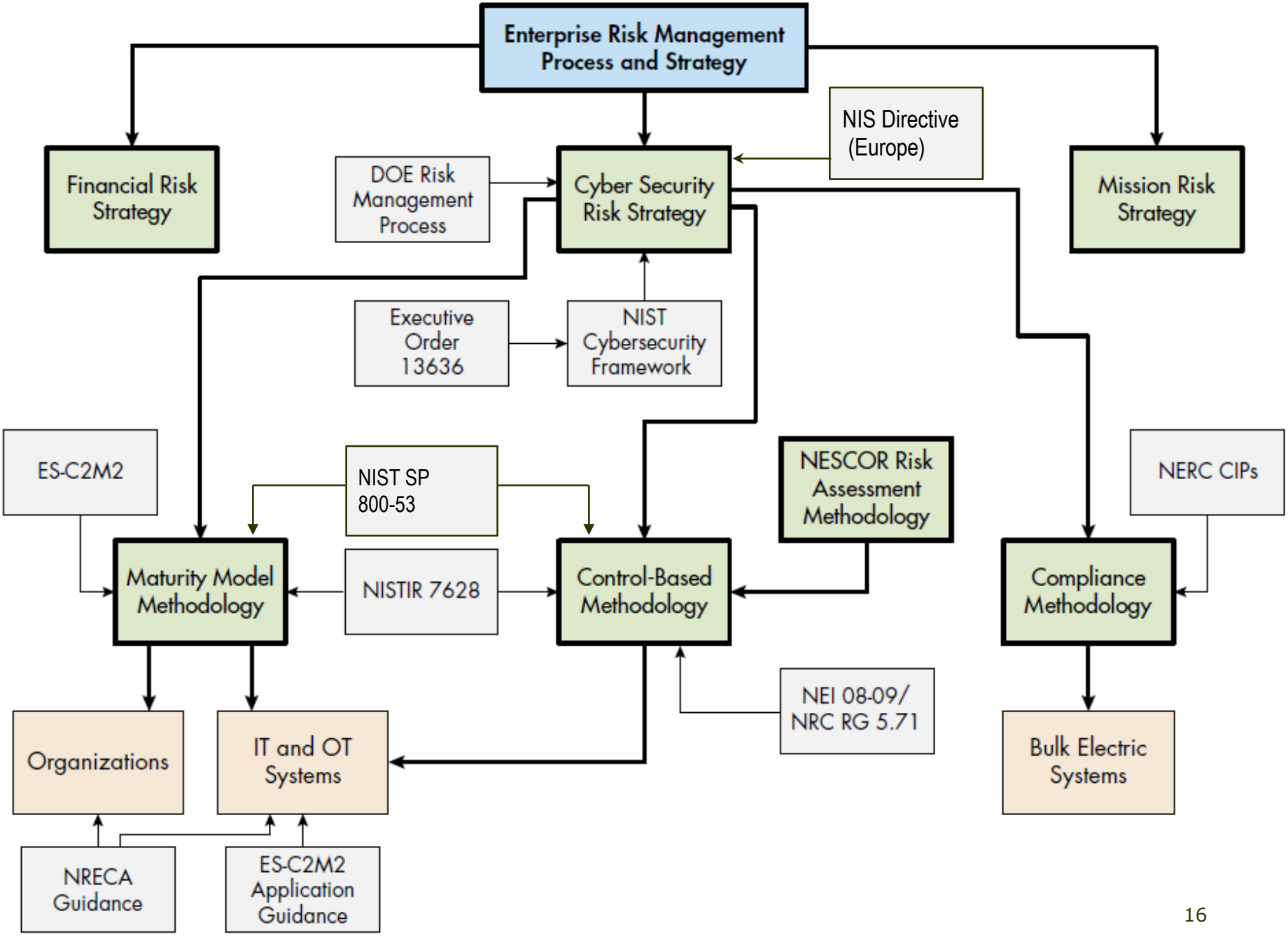
IT and Control Systems – Differences…

- For IT systems, **confidentiality** and **integrity** are the major objectives
- For control systems, **availability** and **integrity** are the major objectives

- Limited bandwidth and processing capability
- Potential loss of life impact if there is a major compromise
- Time critical content
  - For IT, delays are usually accepted
  - For control systems, critical due to safety
- IT system life cycle varies from 6 months to 2 years
- Control systems life cycle varies from 15 to 40 years

Getting Started – Practical *Risk Management*


Risk Assessment Methodology
Asset/System Characterization
Threat Agent Characterization
Vulnerability Assessment
Impact Analysis
Threat Likelihood Assessment
Risk Determination
Security Requirements/ Controls
No
Risk Acceptable?
Yes


Enterprise Risk Management Process and Strategy
Financial Risk Strategy
DOE Risk Management Process
Cyber Security Risk Strategy
NIS Directive (Europe)
Mission Risk Strategy
Executive Order 13636
NIST Cybersecurity Framework
ES-C2M2
NIST SP 800-53
NESCOR Risk Assessment Methodology
NERC CIPs
Maturity Model Methodology
NISTIR 7628
Control-Based Methodology
Compliance Methodology
NEI 08-09/ NRC RG 5.71
Organizations
IT and OT Systems
Bulk Electric Systems
NRECA Guidance
ES-C2M2 Application Guidance

Acronyms….

- CIP: Critical Infrastructure Protection
- DOE: Department of Energy
- ES-C2M2: Electricity Subsector Cybersecurity Capability Maturity Model
- IT: Information Technology
- NEI: Nuclear Energy Institute
- NERC: North American Electric Reliability Cooperation
- NESCOR: National Electric Sector Cybersecurity Organization Resource
- NIS: Network and Information Security
- NIST: National Institute of Standards and Technology
- NISTIR: Interagency Report
- NRC: Nuclear Regulatory Commission
- NRECA: National Rural Electric Cooperative Association
- OT: Operations Technology
- SP: Special Publication

Cybersecurity Capability Maturity Model (C2M2)

Overview

Expansion Project and Comparative Analysis

National Electric Sector Cybersecurity Organization Resource (NESCOR)

Build an industry collaboration

- Public/private partnership funded by DOE
- Utilities, vendors, academia, consultants, regulators

Address critical industry needs

- Failure scenarios and impact analyses

Collaboration across all participants

Describing Failure Scenarios

Example of a Failure Scenario

Malicious Code Injected into Substation Equipment via Physical Access	
Description	What is the incident?
Relevant Vulnerabilities	How does the incident occur?
Impact on Power System	How does it affect survivability/ reliability/resiliency?
Potential Mitigations	How do we reduce the risk?

url: Smartgrid.epri.com/nescor.aspx

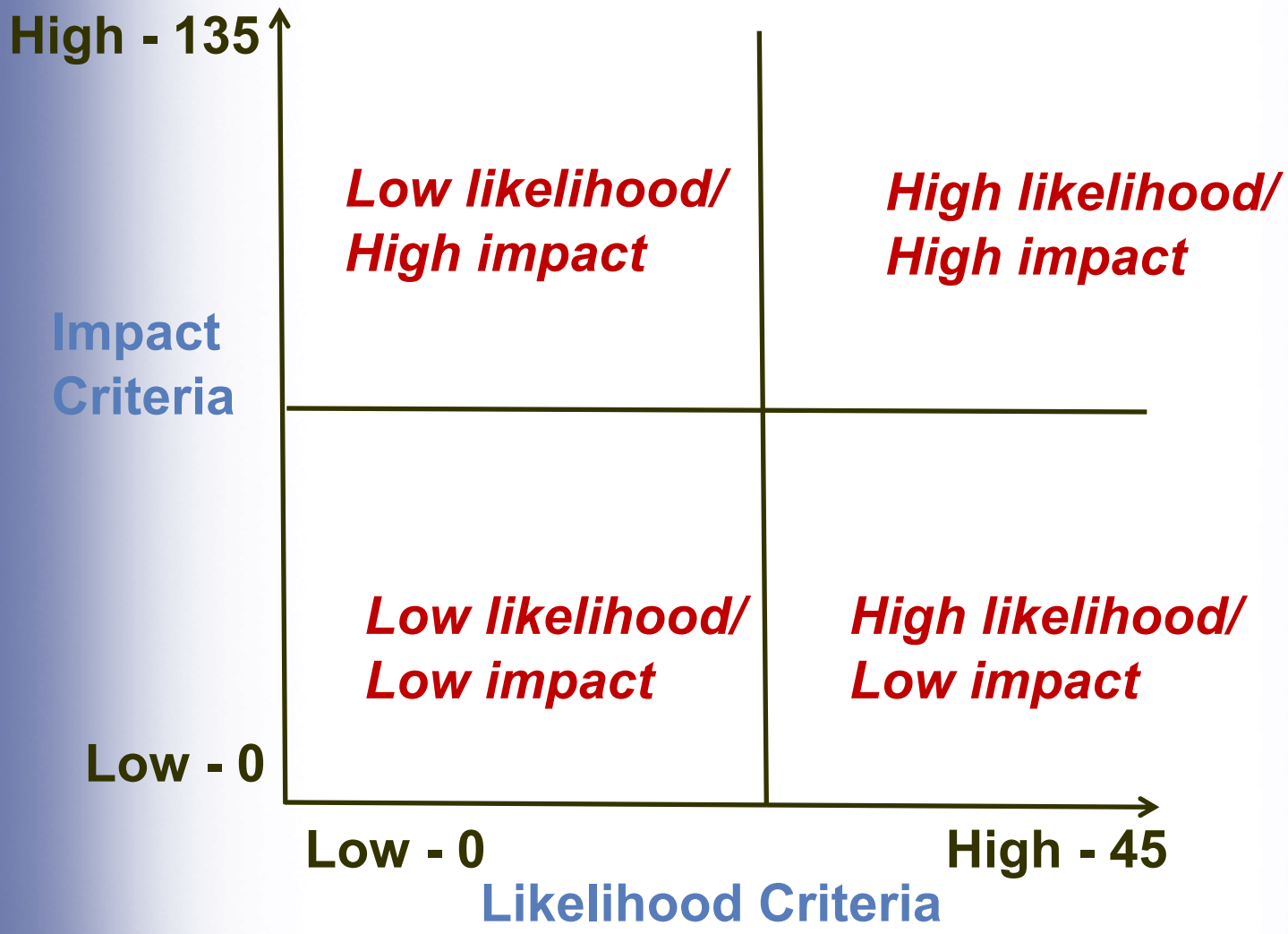
Impact Criteria - Examples

Criterion	How to score
System scale	0: single utility customer, 1: neighborhood, 3: town or city, 9: potentially full utility service area and beyond
Public safety concern	0: none, 1: 10-20 injuries possible, 3: 100 injured possible, 9: one death possible
Financial impact of compromise on utility	0: Petty cash or less, 1: up to 2% of utility revenue, 3: up to 5%, 9: Greater than 5%

Likelihood and Opportunity - Examples

Criterion	How to score
Skill required	0: Deep domain/insider knowledge and ability to build custom attack tools, 1: Domain knowledge and cyber attack techniques, 3: Special insider knowledge needed, 9: Basic domain understanding and computer skills
Common vulnerability among others	0: Isolated occurrence 1: More than one utility, 3: Half or more of power infrastructure, 9: Nearly all utilities
Accessibility (logical, assume have physical access)	0: High expertise to gain access, 1: Not readily accessible, 3: Publicly accessible but not common knowledge, 9: Common knowledge or none needed

Failure Scenarios Risk Ranking Graph



Common Sub Trees

- Threat Agent Gains Capability to Reconfigure <firewall>
- Threat Agent Blocks Wireless Communication Channel Connecting <x and y>
- Authorized Employee Brings Malware into <system or network>
- Threat Agent Obtains Credentials for <system or function>
- Threat Agent Uses Social Engineering to <desired outcome>
- Threat Agent Exploits Firewall Gap in <specific firewall>
- Threat Agent Exfiltrates <data>
- Threat Agent Gains Access to <network>

Common Tree: Threat Agent Gains Access to <network>

Description

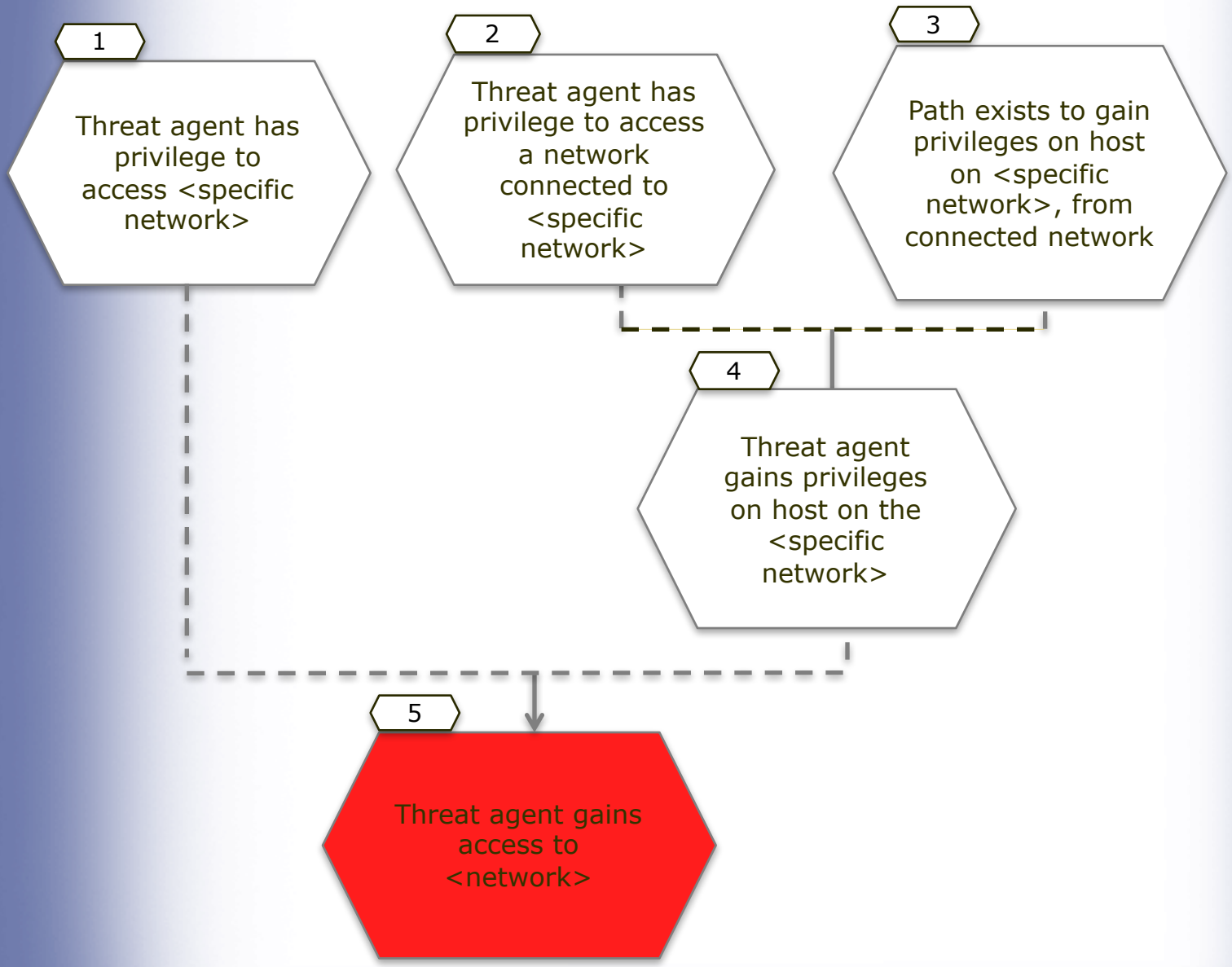
A threat agent becomes capable of sending traffic within a network and attempting to communicate with its resident hosts.

- **Note:** This draft tree currently expresses the high level concept of "bridging" sequentially between adjacent networks. Information should be added in future drafts related to:
  - Mitigations for detecting and preventing network reconnaissance
  - Specific differences in gaining access to networks that use various protocols and technologies

Assumptions

- None currently identified

Common Tree: Threat Agent Gains Access to <network>



Common Tree: Threat Agent Gains Access to <network>

Potential Mitigations

1, 2 - Enforce least privilege to limit individuals with privilege to the network and connected networks

2 - Isolate network

3 - Enforce restrictive firewall rules for access to network

3 - Design for security by limiting connection points to networks that are widely accessible and by limiting number of hosts on same network

3 - Require authentication to the network

4 - Enforce least privilege for individuals with access to hosts on the network

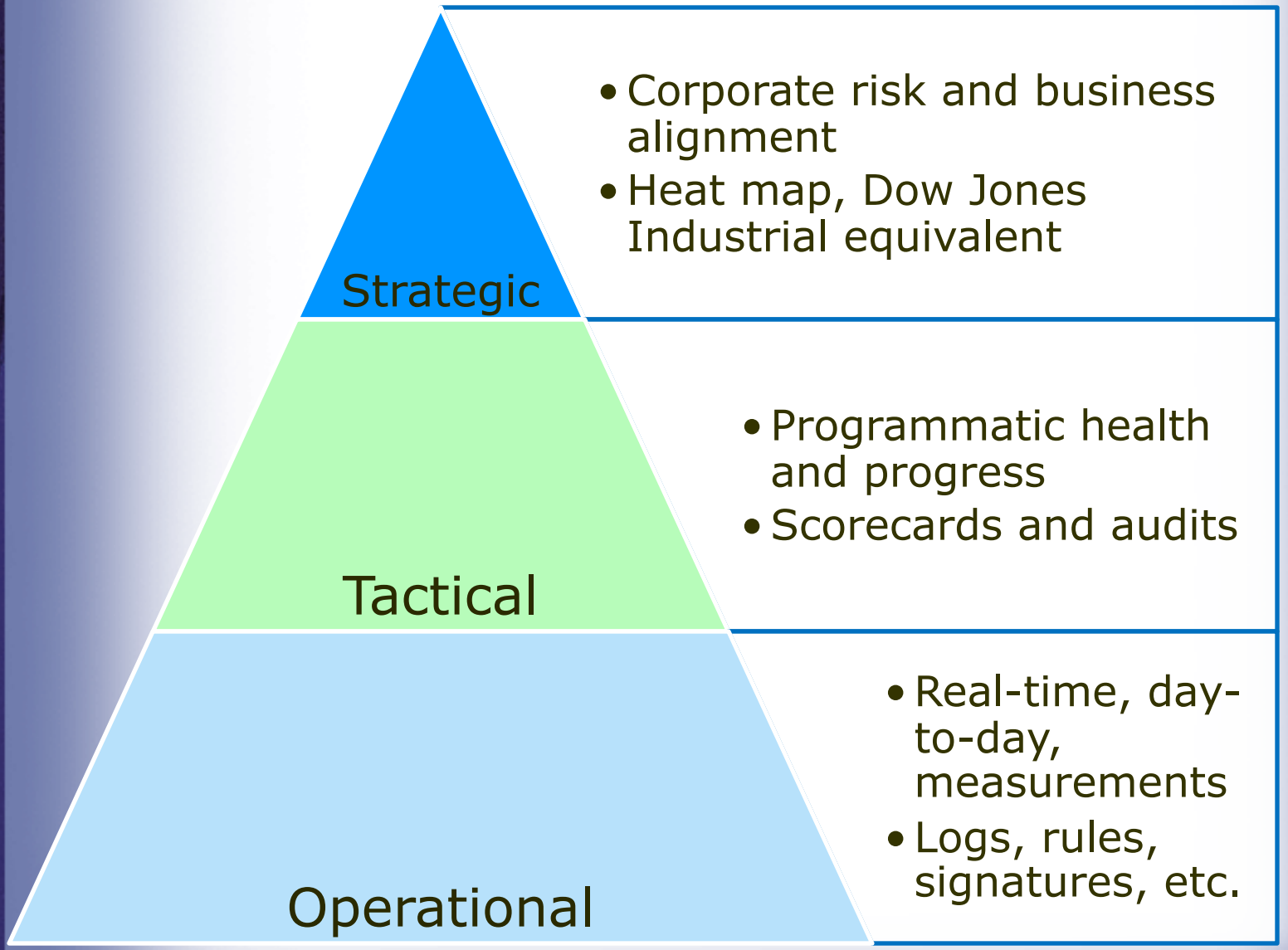
4 - Detect unusual patterns of usage on hosts and network

What's Next?

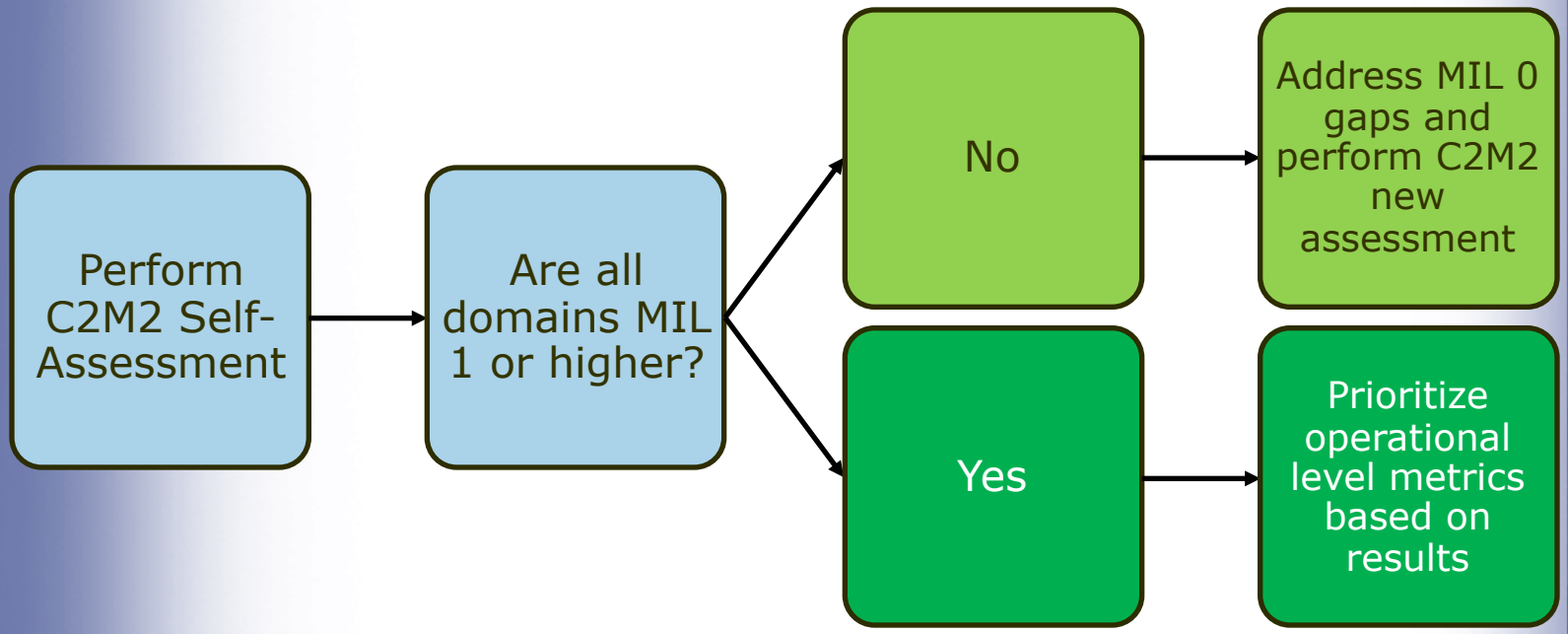
Security Metrics

- Create meaningful and engineering-based security metrics for the electric sector. These metrics must:
  - Be based on quantitative, repeatable data sets
  - Be independent of compliance to mandatory standards
  - Allow for tailoring across the utility, including various business units, functions, and ownership structures
  - Consider differences between IT and OT architectures
  - Communicate the state of cyber security to different stakeholders

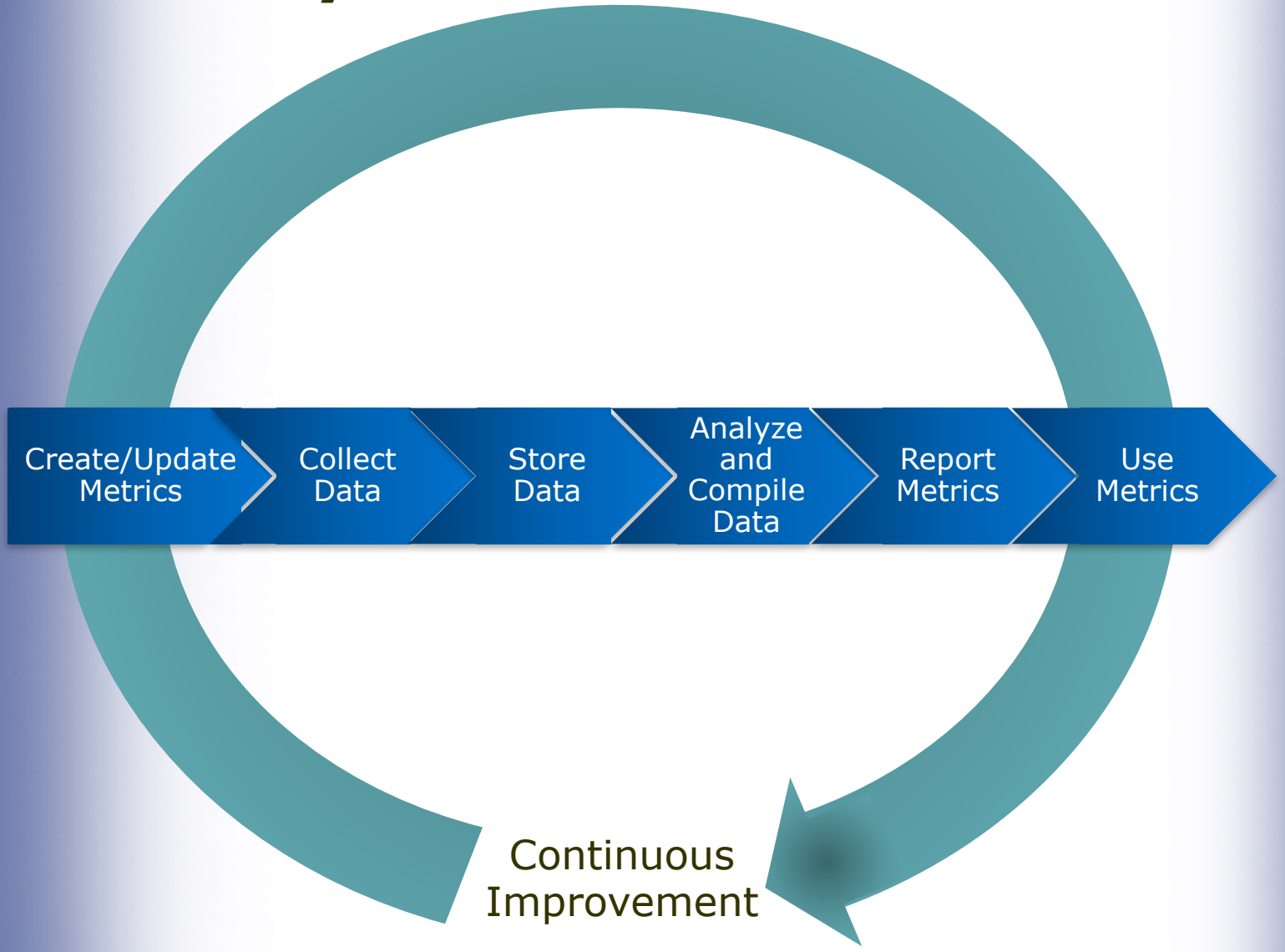
Metrics Across the Organization



Getting Started….



Metrics Cycle



Security Architecture Overview

- Issue
  - As intelligent devices are deployed on the grid, the number of interfaces and associated attack surfaces and attack vectors will increase

- Project approach
  - Identify and assess the attack surface and attack vectors
  - Identify mitigation strategies

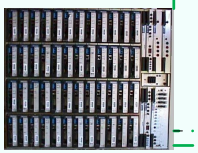
- Requirements
  - Must be *actionable*
    - Manage cyber security risk vs avoiding risk
  - Should provide useful information to senior management

Analog MW System

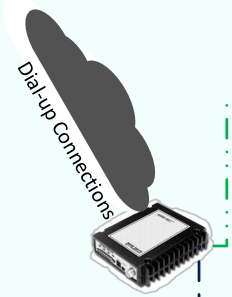
Communications Transport System

Control Center

Digital Cross Connect System



Channel Bank



Dial Modem

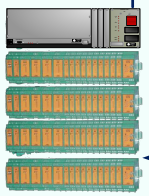
Dial Modem

Dedicated Modem

GPS Clock

Relay Controller

Digital Fault Recorder



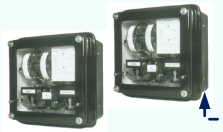
SCADA RTU

Microprocessor Relays

Panel Meters and Transducers

Local Batteries and Power Distribution

Power Line Carrier Terminal



Electromech Relays

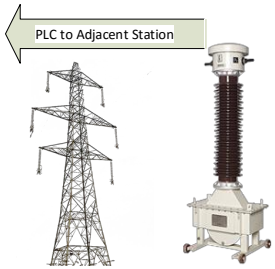
Programmable Logic Controllers

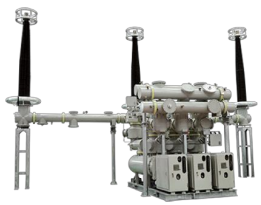
Connection Types

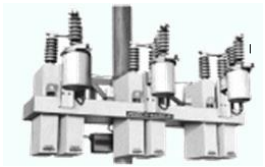
- Analog/TDM
- IRIG-B
- Digital Serial
- Secondary and Control Wiring (Signals)

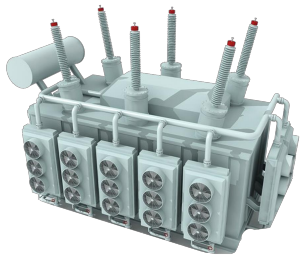
NOTE: All lines shown without arrows are bi-directional communications

Primary Power Equipment



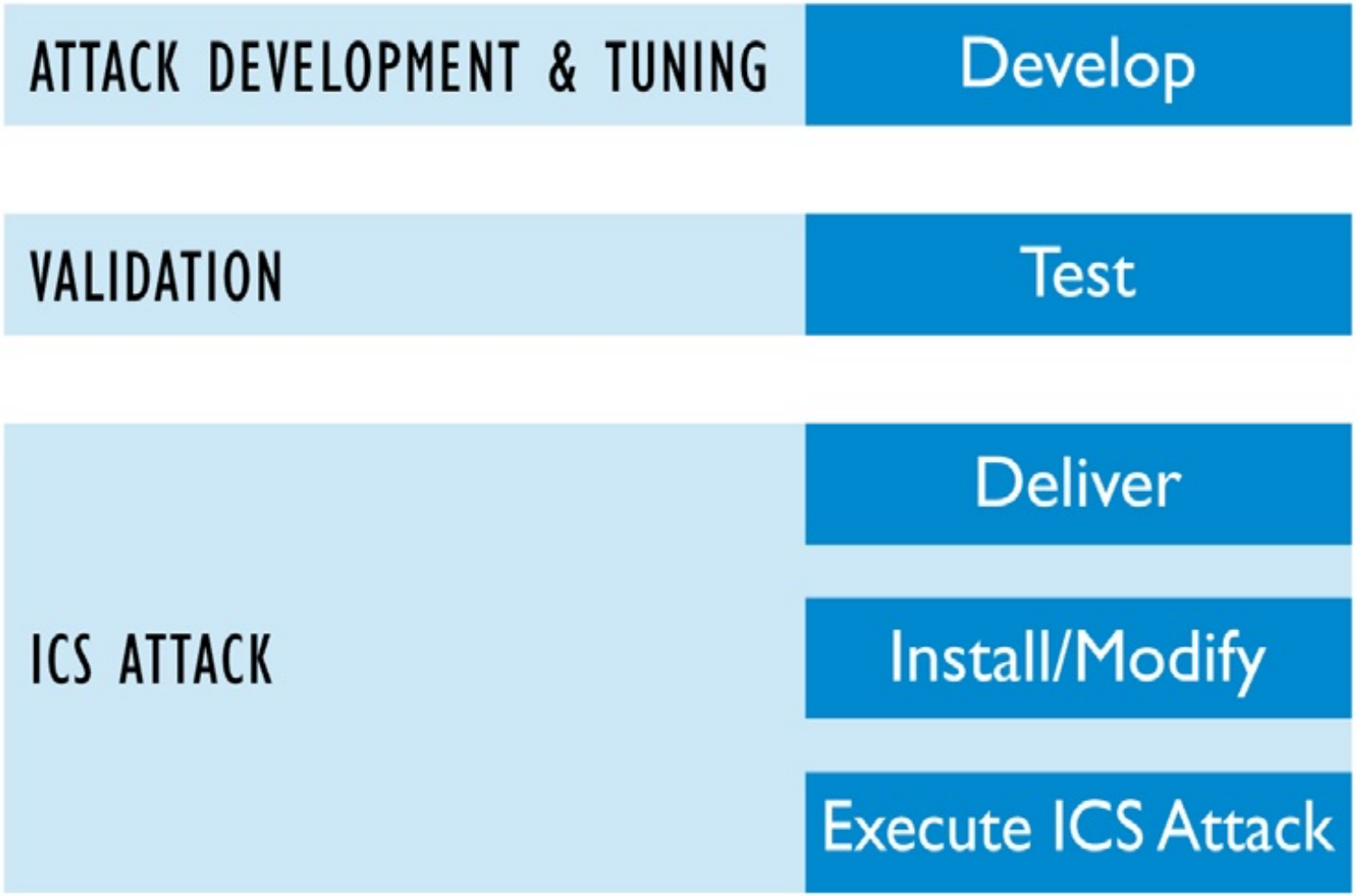






Title	Revision
Legacy Substation Architecture	05/27/2016

SANS ICS Kill Chain



Moving Forward…

- Cyber security supports both the **reliability** and **privacy** of the Smart Grid
- Address **interconnected systems** – both IT and control systems
  - Cyber security needs to be addressed in all systems, not just critical assets
  - Augment existing protection controls, as applicable
- Continuously **monitor and assess** the security status
- Acknowledge will be some security breaches
  - Focus on response and recovery
  - *Fail secure*
    - Address both safety and security

alee@epri.com
202.293.6345

Discussion